JOURNAL OF ALGEBRA, 1, 347-354 (1964)

On Simple Rings Satisfying a Type of "Restricted" Polynomial Identity

M. SLATER

Mathematics Department, University of Chicago, Chicago, Illinois

Communicated by I. N. Herstein

Received June 3, 1964

1. INTRODUCTION

A celebrated result due to Kaplansky [*4*] states that if R is a primitive ring satisfying a polynomial identity over its centroid Z, then R is finite-dimensional over Z. It is natural to wonder what results may be obtained if some of the variables in the polynomial identity have restricted range. Thus Martindale [*7*] considers rings with involution such that a polynomial identity is satisfied on the set of symmetric elements. If A is a subring of a primitive ring R, and if a polynomial identity is satisfied in R whenever certain of its variables are restricted to taking values in A, for example, it may be possible to say something about the nature of A, perhaps when regarded as an algebra over its own center.

In this paper we consider polynomial identities in which only one of the variables is restricted. The restriction we impose is, however, extreme: we insist that the distinguished variable assume a *fixed* value in R. If R is primitive, and this fixed value is the element $a \in R$, our result is that a is algebraic over the centroid Z of R.

Section 2 of this paper gives the necessary precise statement of this result (Theorem 1), and its proof. In Section 3 we consider an example of a "restricted" polynomial identity of the type dealt with in Section 2. This example arises as a natural generalization of identities that have been considered in the literature (see Section 3 for details). As an application of our result of Section 2 we prove that a primitive ring satisfying this restricted polynomial identity is four-dimensional over its center (Theorem 2).

It will be noted that in both our theorems we refer to "simple or primitive" rings. In the classical (finite-dimensional) case these two concepts coincide. However, if we do not impose any chain conditions, there exist primitive rings which are not simple, and since our proofs when R is primitive make no use of simplicity, we prefer the more general formulation. It is also possible for a simple ring to fail to be primitive: in this case it must be a radical ring (i.e., equal to its own Jacobson radical). For an example showing that this can occur see [*8*]. Both of our proofs therefore first dispose of the case where R is a simple radical ring, before treating the case where R is primitive.

2. Restricted Polynomial Identities

Let Z be a field, and $p \neq 0$ a member of the free associative algebra $Z[y, x_1, \cdots, x_t]$ $(t \geq 0)$. We say that R satisfies the *restricted polynomial identity* $p(a, x_1, \cdots, x_t)$ provided R is a ring with centroid containing Z, $a \in R$, and $p(a, b_1, \cdots, b_t) = 0$ for any choice of the $b_i \in R$. We allow p to have a nonzero constant term: in this case R necessarily has a nontrivial center. We shall maintain the distinction between p (a member of a free algebra) and $p(a, x_1, \cdots, x_t)$ (a function on the ring R). We now have

Theorem 1. *Let R be a simple or primitive ring with centroid Z, and suppose R satisfies the restricted polynomial identity $p(a, x_1, \cdots, x_t)$. Then a is algebraic over Z.*

Proof. Let $q \in Z[y, x_1, \cdots, x_s]$ be the polynomial obtained by complete linearization of p on every indeterminate x_i. It is clear that $q \neq 0$, and that R satisfies the restricted polynomial identity $q(a, x_1, \cdots, x_s)$. Thus we may assume without loss, and in future shall assume, that p is linear in every x_i.

(a) Suppose first that R is a simple radical ring. In this case the conclusion of the theorem amounts to saying that a is nilpotent. For otherwise there is a standard method for extracting an idempotent from $Z[a]$, and a radical ring contains no idempotents.

We proceed by induction on t. If $t = 0$ then $0 \neq p \in Z[y]$, $p(a) = 0$ in R, and a is algebraic over Z, as required. Suppose then that we have the result whenever R satisfies a restricted polynomial identity in s variables $(s < t)$, and that $t \geq 1$.

We may write p as a sum $\sum \beta_i \mu_i$ where the μ_i are monomials in y and the x_i. Let $r \geq 0$ be the integer for which no monomial of p ends in y^{r-1}, and at least one monomial ends in y^r. (In particular, $r = 0$ if no monomial ends in y.) Then we may write

$$p(y, x_1, \cdots, x_t) = \sum_{i=1}^{t} p_i \cdot x_i \cdot y^r + p_0 y^{r+1}.$$

Here each p_i is a polynomial in y and the x_j other than x_i (since p is linear in x_i). We may have $p_i = 0$ for some i, but our choice of r forces the existence of at least one k such that $p_k \neq 0$. Let us fix one such k. We now wish to replace each x_i $(i \neq k)$ in p by $x_i y$. Formally, we proceed as follows. Given any $q = q(y, x_1, \cdots, x_t)$ of the free algebra, we define

$$q' = q'(y, x_1, \cdots, x_t) = q(y, x_1 y, x_2 y, \cdots, x_k, \cdots, x_t y).$$

Then

$$p'(y, x_1, \cdots, x_t) = \sum_{i \neq k} p_i' \cdot x_i y \cdot y^r + p_k' \cdot x_k \cdot y^r + p_0' \cdot y^{r+1}$$

$$= p_k' \cdot x_k \cdot y^r + p_1 \cdot y^{r+1} \text{ for some } p_1 .$$

We note that $p_k' \neq 0$ since $p_k \neq 0$, and that x_k does not occur in p_k'.

Suppose now $b_1, \cdots, b_t \in R$ are arbitrary. Set

$$c = p_k'(a, b_1, \cdots, b_t); \qquad d = p_1(a, b_1, \cdots, b_t).$$

Then since R clearly satisfies the restricted polynomial identity $p'(a, x_1, \cdots, x_t)$, we have $c \cdot b_k \cdot a^r + d \cdot a^{r+1} = 0$, or $c \cdot b_k \cdot a^r \in R \cdot a^{r+1}$. Since this relation holds for any choice of $b_k \in R$, and since c is independent of b_k (recollect that x_k does not occur in p_k'), we may write

$$cR \cdot a^r \subseteq R \cdot a^{r+1} \tag{1}$$

Now set $L = \{x : x \in R \text{ and } x \cdot a^r \in R \cdot a^{r+1}\}$. Clearly L is a left ideal. If $L = R$ we have $R \cdot a^r \subseteq R \cdot a^{r+1}$, whence in particular $a^{r+1} = s \cdot a^{r+1}$ for some $s \in R$. But a member s of the radical of a ring can act as the identity only on the zero of the ring. Since R is a radical ring, this shows that we must have $a^{r+1} = 0$, which proves the theorem. Suppose then $L \neq R$. By (1) we have $cR \subseteq L$, so that $cR + RcR \subseteq L + RL = L \neq R$, and since the left side is an ideal, and R is simple, this yields $cR = (0)$, whence $c = 0$, since the left annihilator of R must be the zero ideal. We have thus shown that every value $c = p_k'(a, b_1, \cdots, b_t)$ assumed by the function $p_k'(a, x_1, \cdots, x_t)$ is zero, which is to say that R satisfies the restricted polynomial identity $p_k'(a, x_1, \cdots, x_t)$. Since as we have already seen $0 \neq p_k' \in Z[y, x_1, \cdots, \hat{x}_k, \cdots, x_t]$, the theorem now follows by our inductive hypothesis.

(b) Suppose now that R is a primitive ring. The proof for this case will be a consequence of the lemma below. We first explain our terminology.

Let a be a linear transformation on a vector space W over a field K. We say *a acts algebraically* on an element $v \in W$ provided there exists $q \neq 0$, $q \in K[x]$, such that $v \cdot q(a) = 0$. We say *a is algebraic on* a subspace W_0 of W provided for some $q \neq 0$, $q \in K[x]$, we have $w \cdot q(a) = 0$ for every $w \in W_0$. We say *a is algebraic* provided it is algebraic on W itself. We now have the

LEMMA. *Let a be a linear transformation on a vector space W over a field K, and suppose a is not algebraic. Let U_0 be a basis for a subspace W_0 of W, and suppose a is algebraic on W_0. Then given any $n \geqslant 0$ we may find $u \in W$ such that $\{u, ua, \cdots, ua^n\} \cup U_0$ is a linearly independent set.*

Proof: Since a is not algebraic, $W_0 \neq W$, and we may find $u \in W$, $u \notin W_0$. This gives the case $n = 0$ of the lemma. We now proceed by induction on n. Suppose we have proved the lemma for $n - 1$ (given $n \geqslant 1$), and that U_0 is given. By hypothesis we may choose u so that

$$\{u, ua, \cdots, ua^{n-1}\} \cup U_0 = U_1$$

is a linearly independent set. If the conclusion of the lemma is false, we have $ua^n \in W_1$, the subspace spanned by U_1. So we may write

$$ua^n = \alpha_{n-1}ua^{n-1} + \cdots + \alpha_0 u + w \ (w \in W_0),$$

or $u \cdot p(a) \in W_0$, where $p(a) = a^n - \alpha_{n-1}a^{n-1} - \cdots - \alpha_1 a - \alpha_0$. By hypothesis a is algebraic on W_0. Suppose then $q(a) = 0$ on W_0. Then $p(a) \cdot q(a) = 0$ on W_1. (It is here we use our assumption that K is commutative).

Suppose now $y \notin W_1$. We shall say y is *good* provided

$$\{y, ya, \cdots, ya^{n-1}\} \cup U_1$$

is a linearly independent set. If the conclusion of the lemma is false, we may find $\alpha_i', \alpha_i'' \in K$ (we do not assert they are unique), such that

$$ya^n = \alpha_{n-1}' ya^{n-1} + \cdots + \alpha_0' y + w',$$

$$(u + y)a^n = \alpha_{n-1}''(u + y)a^{n-1} + \cdots + \alpha_0''(u + y) + w''$$

for some $w', w'' \in W_0$. Using the fact that y is good we now see that $\alpha_i' = \alpha_i''(0 \leqslant i \leqslant n - 1)$, and then using the fact that U_1 is a linearly independent set we see also that $\alpha_i' = \alpha_i$. Thus $\alpha_i = \alpha_i'$, whence $y \cdot p(a) = w'$. So if y is good we have shown that $y \cdot p(a)q(a) = 0$. Thus $p(a) \cdot q(a) = 0$ on the subspace W_2 spanned by W_1 and all the good elements of W. Let U_2 be a basis for W_2, and suppose $z \notin W_2$. Since z is not good,

$$\{z, za, \cdots, za^{n-1}\} \cup U_1$$

is not a linearly independent set. *A fortiori* $\{z, za, \cdots, za^{n-1}\} \cup U_2$ is not a linearly independent set. Since this is true for any $z \notin W_2$, and since a is algebraic on W_2, the conclusion of the lemma (with $n - 1$ for n, U_2 for U_0, and W_2 for W_0) fails. By our inductive hypothesis, the premiss must also fail, which is to say that a is algebraic after all.

We return now to the proof of the theorem. Let K be an extension of Z which splits R (see for example [3], p. 120), and form $R' = R \otimes_Z K$. Then

R' may be represented as a dense ring of linear transformations on a vector space W over K. Since p is linear in each of its variables, p is inherited by R' (provided we understand a to mean $a \otimes 1$). We aim to show a (in R') is algebraic over K.

Now p, as before, may be regarded as a sum $\sum \beta_i \mu_i$, where each $\beta_i \in Z$ and each μ_i is a string of x_j's and y's. Let r be the maximal number of times y appears in succession in any one of the μ_i, and let t, as before, be the number of distinct x_j appearing in p. We proceed to construct a linearly independent set

$$U = \{u_0, u_0a, \cdots, u_0a^r; u_1, u_1a, \cdots, u_1a^r; \cdots; u_t, u_ta, \cdots, u_ta^r\}.$$

If a acts algebraically on every element of W, then a is algebraic on every finite-dimensional subspace of W, and we may construct U by successive applications of the lemma, starting from $U_0 = \phi$. If a does not act algebraically on every element of W, we may find $u \in W$ such that $\{u, ua, ua^2, \cdots\}$ is a linearly independent set. In this case we may construct U by setting $u_i = ua^{(r+1)i}$.

Let us say the *degree* of a monomial μ of p is the total number of x_i's and y's occurring in it (for example, $x_2yx_4x_3y^2$ has degree 6). Choose μ_0 of maximal degree in p, and suppose (without loss of generality) that

$$\mu_0 = y^{r_0}x_1y^{r_1}x_2 \cdots x_sy^{r_s} \qquad (0 \leqslant r_i \leqslant r;\ s \leqslant t).$$

By the density of R we may now choose $e_i \in R(1 \leqslant i \leqslant t)$ so that

$$(u_ia^{r_i})e_i = u_{i+1} \qquad (0 \leqslant i < s);$$
$$ve_{i+1} = 0 \text{ for } v \in U \text{ otherwise } (1 \leqslant i \leqslant t).$$

We proceed to examine the action of $p(a, e_1, \cdots, e_t)$ on u_0. If λ is an initial segment of any monomial μ of $p(a, e_i)$, it is clear that $u_0\lambda \in U$, and moreover that $u_0\lambda = 0$ unless λ is of the form νa^m, where ν is an initial segment of μ_0. Thus we may write

$$u_0 \cdot p(a, e_i) = \sum_{i<s} \beta_i u_i a^{m_i} + \beta u_s a^{r_s}, \tag{2}$$

where the first terms arise from those monomials of p, other than μ_0, which do not annihilate u_0, and the last term arises from μ_0. Since β, the coefficient of μ_0, is by hypothesis nonzero, and $u_sa^{r_s}$ is independent of the other terms in (2), $p(a, e_i)$ cannot act as the zero transformation on u_0, contradicting our assumption that in R' $p(a, x_1, \cdots, x_t) = 0$. We have thus shown that a (or rather $a \otimes 1$) must be algebraic over K. But then

$$\infty > [K[a \otimes 1] : K] = [Z(a) \otimes_Z K : K] = [Z(a) : Z],$$

so that a is algebraic over Z, the required conclusion.

3. Rings Satisfying a Certain Identity

As an example of a "restricted" polynomial identity of the type we have been considering, we may note that Herstein [2] required the following result:

If R is simple of characteristic 2 with center Z, $a \notin Z$ is an element of R such that $a^2 \in Z$, and $(ax - xa)^2 \in Z$ for all $x \in R$, then $[R : Z] = 4$.

Baxter [1] proved a similar result, but with exponent 4 instead of 2.

Here the relevant polynomial $p \in Z[y, x_1, x_2]$ is

$$p(y, x_1, x_2) = x_1(yx_2 - x_2y)^4 - (yx_2 - x_2y)^4x_1 .$$

In this section we show that all the restrictions in the statement of this result are unnecessary. Specifically, we prove

Theorem 2. *Let R be a simple or primitive ring with center Z. Suppose there exists $a \in R$, $a \notin Z$ such that*

$$(ax - xa)^n \in Z \tag{3}$$

for all $x \in R$ and some fixed $n > 0$. Then $[R : Z] = 4$.

It should be noted that we did not assume R has a *nontrivial* center. That it does follows from the conclusion, since a finite-dimensional simple (or primitive) ring has a unity.

Since a semisimple ring is a subdirect sum of primitive rings, we have the

Corollary. *If R is semisimple and satisfies (3) for some $a \in R$, all $x \in R$ and fixed $n > 0$, then $(ax - xa)^2 \in Z$ for all $x \in R$.*

For if R_i is a primitive component of R, then either the projection a_i of a into R_i is central, or by the theorem $[R_i : Z_i] = 4$, and in either case $(a_ix_i - x_ia_i)^2 \in Z_i$ for all $x_i \in R_i$. The result then follows on sticking the pieces together.

We turn now to the proof of Theorem 2.

(a) Suppose first that R is a simple radical ring. We aim to show that this case cannot arise. By Theorem 1, a is nilpotent. Suppose then $a^{r+1} = 0$, $a^r \neq 0$. Set $b = a^r$. Then given $x \in R$ we have $bx - xb = a^rx - xa^r = ay - ya$, where $y = a^{r-1}x + a^{r-2}xa + \cdots + xa^{r-1}$. Thus $(bx - xb)^n \in Z$ for all $x \in R$, and since a radical ring has trivial center, $(bx - xb)^n = 0$ for all $x \in R$. Since $b^2 = 0$, we find $0 = (bx - xb)^nb = (bx)^nb$, and $(bx)^{n+1} = 0$ for all $x \in R$. Thus bR is a nil right ideal of bounded index. By [6] (see also [2], pp. 281–282), this cannot occur in a simple ring unless $bR = (0)$. But then $b = 0$, contradicting our definition of b. Thus R is not a radical ring.

(b) Suppose now that R is a primitive ring. Then R is representable as a dense ring of linear transformations on a vector space V over a division ring D.

We assume such a representation, taking V to be a left vector space, and the transformations to act from the right.

Suppose first that we may find $v, w \in V$ such that v, va, w are linearly independent over D. Let W be the subspace of V spanned by these three vectors. Then either $wa \notin W$, or there exist $\alpha, \beta, \gamma \in D$ such that

$$wa = \alpha v + \beta va + \gamma w.$$

In either case we may by density choose $b \in R$ so that

$$vb = 0, \quad (va)b = v, \quad wb = 0, \quad (wa)b = \beta v.$$

(If $wa \notin W$ we may choose β arbitrarily). Then we may verify that

$$v(ab - ba)^n = v; \qquad w(ab - ba)^n = \beta v \neq w,$$

so that $(ab - ba)^n$ cannot be central.

There remain two possibilities: for all $u \in V$, u and ua are linearly dependent, or there exists $v \in V$ such that $\{v, va\}$ forms a basis for V.

In the second case, given $\beta \in D$, choose $b \in R$ so that

$$vb = 0; \qquad (va)b = \beta v.$$

Such a choice is possible by density. Then $v(ab - ba)^n = \beta^n v$, whence for all $\beta \in D$ we have $\beta^n \in Z$. But then by [5] $D = Z$, and R is the two by two matrices over Z. This gives us the split case of the theorom.

Suppose now that u and ua are linearly dependent for every $u \in V$. We aim to show V is one-dimensional over D. If not, we may find $v, w \in V$ linearly independent over D. Suppose

$$va = \alpha v; \qquad wa = \gamma w.$$

Given an arbitrary $\beta \in D$ we may by density choose $b \in R$ so that

$$vb = \beta v; \qquad wb = 0.$$

Then $w(ab - ba)^n = 0$, and since $(ab - ba)^n$ is central, this yields $(ab - ba)^n = 0$. But $v(ab - ba)^n = (\alpha\beta - \beta\alpha)^n v$, so that $(\alpha\beta - \beta\alpha)^n = 0$, whence $\beta\alpha = \alpha\beta$. Since β was arbitrary, this shows that $\alpha \in Z$.

If $u \in V$ is arbitrary we may show similarly that $ua = \delta u$, for some $\delta \in Z$. If u is linearly dependent on v *over* Z, then clearly $\delta = \alpha$. If not, we may use the relation

$$(u + v)a = \epsilon(u + v), \quad \text{some} \quad \epsilon \in Z,$$

to obtain the same result.

We thus see that $ua = \alpha u$ for all u and a certain $\alpha \in Z$; that is, a is central. This contradiction shows that V is one-dimensional, or in other words R is a division algebra.

Suppose first Z is infinite. Then if K is any extension of Z, the ring $R' = R \otimes_Z K$ inherits the restricted identity (3), provided we read "K" for "Z" and "$a \otimes 1$" for "a." The proof is by a standard argument using a Vandermonde determinant. Now by Theorem 1 a is algebraic over Z. Suppose then q is its minimum polynomial. Then we may choose K to split q over $Z : K = Z[\beta]$, $q(\beta) = 0$ in K. Then $a \otimes 1 - \beta$ is a zero-divisor in R', so that R' is not a division ring. But R' is simple with nontrivial center, and so is certainly primitive. Thus by our previous result $[R' : K] = 4$. But then $[R : Z] = [R' : K] = 4$, and this gives us the division ring (quaternion) case of the theorem.

Suppose finally R is a division ring and Z is finite. Since a is algebraic over Z, we may find $m > 0$ such that $a^{p^m} = a$ (where p is the characteristic of Z). Then (compare [3], p. 183) there exists $b \in R$ such that $b^{-1}ab = a^i \neq a$ (for some i), or $ab = ba^i$.

Set $c = ab - ba \neq 0$. Then

$$ac = a \cdot ab - ab \cdot a = aba^i - ba^i a = (ab - ba)a^i = ca^i.$$

Let P be the subring of R generated by Z, a, c. In view of the facts that Z is finite, $a^{p^m} = a$, $c^n \in Z$, $ac = ca^i$, it is clear that P is finite. But a subring of a division ring is cancellative, and a finite cancellative ring is a division ring. Thus P is a division ring. Since a finite division ring is commutative, we conclude in particular that $ac = ca$. This contradiction shows that if R is a division ring Z cannot be finite, and completes the proof of the theorem.

Acknowledgment

I would like to thank Professor Herstein for the interest and encouragement he has accorded this work.

References

1. Baxter, W., Lie simplicity of a special class of associative rings I. *Proc. Am. Math. Soc.* **7** (1958), 855–863.
2. Herstein, I. N., On the Lie and Jordan rings of a simple, associative ring. *Am. J. Math.* **77** (1955), 279–285.
3. Jacobson, N., Structure of rings. *Am. Math. Soc. Colloq. Publ.* **37**.
4. Kaplansky, I., Rings with a polynomial identity. *Bull. Am. Math. Soc.* **54** (1948), 575–580.
5. Kaplansky, I., A theorem on division rings. *Can. J. Math.* **3** (1951), 290–292.
6. Levitzki, J., On a problem of A. Kurosch. *Bull. Am. Math. Soc.* **52** (1946), 1003–5.
7. Martindale, W. S., Primitive algebras with involution. *Pacific J. Math.* **11** (1961), 1431–1441.
8. Sasiada, E., On the existence of a simple radical ring. *Bull. Acad. Polon. Sci.* **9**, no. 4 (1961), 257.